(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
12 mai 2005 (12.05.2005)

PCT

(10) Numéro de publication internationale
WO 2005/043382 A1

(51) Classification internationale des brevets[7] : G06F 7/58

(21) Numéro de la demande internationale :
PCT/FR2004/050510

(22) Date de dépôt international :
18 octobre 2004 (18.10.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0312435 24 octobre 2003 (24.10.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'activité de Gémenos, F-13420 GEMENOS (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **JOYE, Marc** [BE/FR]; Traverse des Jardins, F-83640 Saint Zacharie (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** METHOD AND ASSOCIATED DEVICE FOR GENERATING RANDOM NUMBERS AT A GIVEN INTERVAL IN TIME

(54) **Titre :** PROCEDE ET DISPOSITIF ASSOCIE DE GENERATION DE NOMBRES ALEATOIRES DANS UN INTERVALLE DONNE

(57) **Abstract:** The invention relates to a cryptographic method wherein a random number generator producing random numbers S_i whose size N is fixed between 0 and W-1 is used to produce a random number R between 0 and a predefined limiter K. According to the invention: E31: a random variable S_i is produced, ranging from 0 -W-1, E32: if the random variable S_i is strictly lower than a coefficient K_i of the limiter K in base W, the coefficient R_i of order i of the random number R is equal to the random number S_i then, for all orders j which are lower than i, a random variable S_j of 0 - W-1 is produced and $R_j = S_j$. E33: unless, if said random variable is greater than coefficient K_i of position i of the limiter K in base W, whereupon said coefficient R_i is determined on the basis of the random variable Si of order i according to a predetermined function, then a coefficient R_{i-1} is determined for the random number R of order i-1 which is immediately lower by repeating stages E31 - E33. The invention also relates to an electronic component which is adapted for implementation of said method and a chip card with said component integrated therein. The invention can be applied to cryptographic calculation.

(57) **Abrégé :** L'invention concerne un procédé cryptographique, au cours duquel on utilise un générateur de nombres aléatoires produisant des nombres aléatoires S_i de taille N fixée compris entre 0 et W-1, pour produire un nombre aléatoire R compris entre 0 et une borne K prédéfinie. Selon l'invention : E31 : on produit une variable aléatoire S_i comprise entre 0 et W-1, E32 si la variable aléatoire S_i est strictement inférieure à un coefficient K_i de la borne K dans la base W, alors le coefficient R_i de rang i du nombre aléatoire R est égal à la variable aléatoire S_i puis, pour tout rang j inférieur à i, on produit une variable aléatoire S_j entre 0 et W-1 et on pose $R_j = S_j$. E33 : sinon, si la dite variable aléatoire est supérieure au coefficient K_i de rang i de la borne K dans la base W, alors on détermine le dit coefficient R_i à partir de la variable aléatoire Si de rang i selon une fonction prédéfinie, puis on détermine un coefficient R_{i-1} du nombre aléatoire R de rang i-1 immédiatement inférieur en répétant les étapes E31 à E33. L'invention concerne également un composant électronique adapté pour la mise en couvre du procédé, et une carte à puce intégrant un tel composant.

WO 2005/043382 A1